Resolving vulnerability identification errors using security requirements on business process models

Resolving Vulnerability Identification Errors using Security Requirements on Business Process Models

Purpose - In any information security risk assessment, vulnerabilities are usually identified by information-gathering techniques. However, vulnerability identification errors - wrongly identified or unidentified vulnerabilities - can occur as uncertain data are used. Furthermore, businesses' security needs are not considered sufficiently. Hence, security functions may not protect business assets sufficiently and cost-effectively.

Design/methodology/approach - This paper aims to resolve vulnerability errors by analysing the security requirements of information assets in business process models. Business process models have been selected for use, because there is a close relationship between business process objectives and risks. Security functions are evaluated in terms of the information flow of business processes regarding their security requirements. The claim that vulnerability errors can be resolved was validated by comparing the results of a current risk assessment approach with the proposed approach. The comparison is conducted both at three entities of an insurance company, as well as through a controlled experiment within a survey among security professionals.

Findings - Vulnerability identification errors can be resolved by explicitly evaluating security requirements in the course of business; this is not considered in current assessment methods.

Research limitations/implications - Security requirements should be explicitly evaluated in risk assessments considering the business context. Results of any evaluation of security requirements could be used to indicate the security of information. The approach was only tested in the insurance domain and therefore results may not be applicable to other business sectors.

Originality/value - It is shown that vulnerability identification errors occur in practice. With the explicit evaluation of security requirements, identification errors can be resolved. Risk assessment methods should consider the explicit evaluation of security requirements.

1. INTRODUCTION

Nowadays, companies rely heavily on information technology (IT) systems to achieve their business objectives, making them vulnerable to IT security incidents. Vulnerability can be defined as "a flaw or a weakness in system security procedures, design, implementation, or internal controls that could be exercised and result in a security breach or a violation of the system's security policy" (Stoneburner et al., 2002). In information security, risk assessment security experts have to rely on uncertainties for threat and vulnerability identification, such as threat lists or security-related best practices; this approach often leads to errors in identification (Fenz and Ekelhart, 2011). Vulnerability identification errors occur when a vulnerability is either wrongly identified or unidentified. These vulnerability identification errors can lead to ignoring substantial weaknesses, or investing in inefficient security measures due to wrongly identified

vulnerabilities. Security reports (CSI, 2009, Verizon, 2010) indicate that flaws in security functions and operations still cause losses due to errors in identifying vulnerabilities that are deliberately exploited.

As a first step in any information security risk assessment, assets, threats and vulnerabilities are identified according to standards from Standards Australia/Standards New Zealand Committee (AS/NZS), the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) such as: AS/NZS ISO 31000 (ASNZ, 2009) (formerly AS/NZS 4360 (ASNZ, 1999) and including ISO/IEC 31000 (ISO, 2009)); ISO/IEC Guide 73 (ISO, 2002); ISO/IEC 27001 (ISO, 2005a) and ISO/IEC 27005 (ISO, 2011). The ISO/IEC 13335-1 (ISO, 2004) defining basic security concepts was replaced by ISO/IEC 2700x series. The determination of business processes (Khanmohammadi and Houmb, 2010) and information assets (Stevens, 2005) was proposed to establish an asset and its value for an organization, while security requirements were introduced (Gerber et al., 2001) to identify the criticality of an asset, the impact of the risks and vulnerabilities, as well as the most suitable security mitigations. But the methods or guidelines used for vulnerability identification based on common or public security practices do not consider enough companies' specific security requirements (Siponen and Willison, 2009) and security requirements are not explicitly evaluated for discovering and resolving vulnerabilities.

In this paper, a new method for resolving vulnerability identification errors is proposed - namely explicitly evaluating security requirements of information assets at business process models. For each information asset identified in key business processes, the criticality in the form of security objectives has to be determined. Then, requirements for the security objectives have to be elicited and are used to argue for the accurate identification of vulnerabilities. In the business process model the entry, processing and communication of information assets are identified. At these process points, it is determined whether the information asset's security requirements are adhered to, with regard to security functions. Any non-adherence represents a vulnerability (in other words, a risk, as in this paper risk is defined as "the non-adherence to security requirements causing harm to the organization"). The novelty is the explicit evaluation of security requirements against the security functions of business process activities, to identify vulnerabilities and their business criticality. Through this procedure, vulnerability identification errors could be resolved, as business security needs and corresponding security functions are explicitly evaluated in the course of operation. Furthermore, security requirements can be used as criteria for result accuracy and the security of information, as security requirements define the desired security (Haley et al., 2004). This has not yet been considered in risk assessment procedures.

In a controlled experiment (as part of a survey conducted among 55 security professionals at a security conference) it was observed that 20% more errors in vulnerability identification occur in cases where security requirements were not considered. In other words, vulnerability identification has been more accurate where security requirements were considered.

Furthermore, an analysis of the risk assessment results of the proposed approach in this paper compared to an approach based on the National Institute of Standards and Technology (NIST) Special Publication

(SP) 800-30 (Stoneburner et al., 2002) and Control Objectives for Information and Related Technologies (COBIT) (ITGI, 2007), applied across three insurance companies at the same time, shows that security issues were identified at least 18% more accurately. Particularly, business process-related issues were identified more effectively; these are more significant risks for a company (Khanmohammadi and Houmb, 2010).

The main contribution of this paper is its demonstration that vulnerability identification errors occur in practice, and that a security requirement- and process model-based approach can improve the accuracy of vulnerability identification. The remainder of the paper is structured as follows: section 2 gives background on information security risk assessments; section 3 provides a theoretical background for the research, as well as explaining the approach in detail. In section 4, validation results are presented and discussed. Section 5 is about related work while the paper is concluded with a summary in section 6.

2. BACKGROUND: INFORMATION SECURITY RISK ASSESSMENT

ISO/IEC 31000 (ISO, 2009), ISO/IEC Guide 73 (ISO, 2002), ISO/IEC 27001 (ISO, 2005a) and ISO/IEC 27005 (ISO, 2011) form the basis of any domain-specific information security (IS) risk assessment standard, as well as of developed IS risk assessment approaches. These standards specify that in the risk assessment phase vulnerabilities should be identified with questions such as "what can happen?" and "how and why can this happen?" by using brainstorming, security testing, checklists and best practices. For example in ISO/IEC 27005, vulnerabilities are determined by known threats, the asset list and existing controls using e.g. vulnerability lists or security testing. Asset valuation, for example by costs incurred by a loss, is used to determine the security value of the asset. Determining the scope, boundaries and criteria of information security management, referred to as context establishment in ISO/IEC 27005, is not discussed in this paper as the focus is on the risk assessment part of the IS risk management process.

Requirements engineering (RE) approaches such as that of Franqueira et al., 2011) show that arguing and reasoning of security requirements can be used to identify implementation and design vulnerabilities, as well as risks. In current IS risk assessment approaches (see section 5 related work), based on the standards mentioned previously, vulnerabilities are identified by known threats, security practices or vulnerability lists. But this method of vulnerability identification - comparing security practices or vulnerability lists against the current security functions – can only prove the presence of vulnerabilities, but not their absence (Wang, 2005). IS risk assessment approaches that define security requirements only use them to determine the impact and consequences of vulnerabilities. However, a statement about security - the true, accurate value of a measurement system (Viera and Garrett, 2005) - cannot be made, because the security needed is not explicitly evaluated in the assessments and vulnerability identification errors can occur. It is hypothesised that with an explicit evaluation of security requirements at business process models, vulnerability identification errors can be resolved, which occur in practice, and a statement about the security of information assets can be provided as the closeness to the accurate value is determined.

3. BUSINESS PROCESS MODEL-BASED IT SECURITY RISK ASSESSMENT

An information security risk assessment should consider both organizational and technological issues (von Solms and von Solms, 2005), providing a company-wide view of risk both as a baseline for improvement, as well as a statement of security. By using business process models and evaluating security requirements of information assets, one can consider organizational issues as well as identify technological issues and provide a statement of security. Information assets can be described as information handled by systems or people residing in facilities of organizations. The proposed approach differs at the vulnerability identification phase to current risk identification procedures, as information assets' security requirements against security functions are evaluated (instead of using a list of vulnerabilities or security best practices).

3.1. *Overview of the proposed approach*

The approach consists of six steps, organized into four phases, namely asset identification, asset profiling, vulnerability identification and document risks. The first phase is identifying critical assets. The second phase is defining security objectives and requirements for the assets. The third phase involves evaluating the assets vulnerabilities. Finally, the vulnerabilities and risks are documented. Figure 1 shows the assessment phases and steps; a rectangle represents a step in the assessment process and the arrows indicate the order of the steps.

In the first phase, 'asset identification', information assets (Stevens, 2005) are identified with the help of business process models of the company's critical business processes. Business process models describe a structured flow of activities of actors (e.g. a human or machine), and applications (systems that perform or support an activity) using information assets (data) embedded in an environment (e.g. an organization or facilities) (zur Muehlen, 2005). These information asset-representing business transactions can be identified by what information is used by actors or applications. Although, Phase one is completed once information assets are identified, it does not necessarily require the identification of all assets at the first attempt. This activity can be restarted or applied iteratively.

In the second phase, 'asset profiling', security objectives and requirements are defined for each information asset. This profiling step establishes clear boundaries for the security required, with regard to the processing of information, containers handling the information asset in a process and security processes applied - as well as when a vulnerability becomes a risk. Security objectives can be defined as a high-level description of the security to be achieved, whilst security requirements are refinements of the security objectives as the constraints required for the system to be satisfied (Mead et al., 2005). Artifacts that can be used include the companies' security policy, organizational procedures, as well as security best practices. The verification of security requirements with regard to validity and correctness is no objective. Any dependencies and inconsistencies between the security needs of information assets can be identified by defining and aligning the security requirements for different business processes in which the information asset is used.

In the third phase, 'vulnerability identification', the information asset security objectives and requirements with regard to implemented security functions are evaluated on the basis of entry, process and communication points in the business process model. An entry, process and communication point is an activity by an actor or system in the process, where an information asset is created, processed or transmitted. With the evaluation of the asset's security objectives at entry, process and communication points, the secure processing (entry, processing and transmission) of the information is determined. With the evaluation of the asset's security requirements at the containers (systems, actors and the environment), the secure handling of the information is determined. Containers are systems, actors or the environment utilizing the information asset or where information resides. It is postulated that - if security requirements are not implemented, not implemented correctly, or not adhered to – it has a negative impact upon the security objective and ultimately upon the business requirements and the organization as a whole. Therefore, a risk and vulnerability can be identified by a deviation from, or non-adherence to, the security requirement by implemented security functions. Security objectives are evaluated by predefined security functions like access control or encryption whereas security requirements by their implementation. The assessment is completed when all entry, process and communication points of the process are evaluated. Information asset identification can be restarted or applied iteratively (the arrow between step 3.2 and 1.2), if a new asset is identified in the vulnerability identification phase.

In the fourth phase, 'document risks', vulnerabilities and the information assets at risk are acknowledged for each business process. The assessment is completed by documenting the vulnerabilities and risks affecting an information asset.

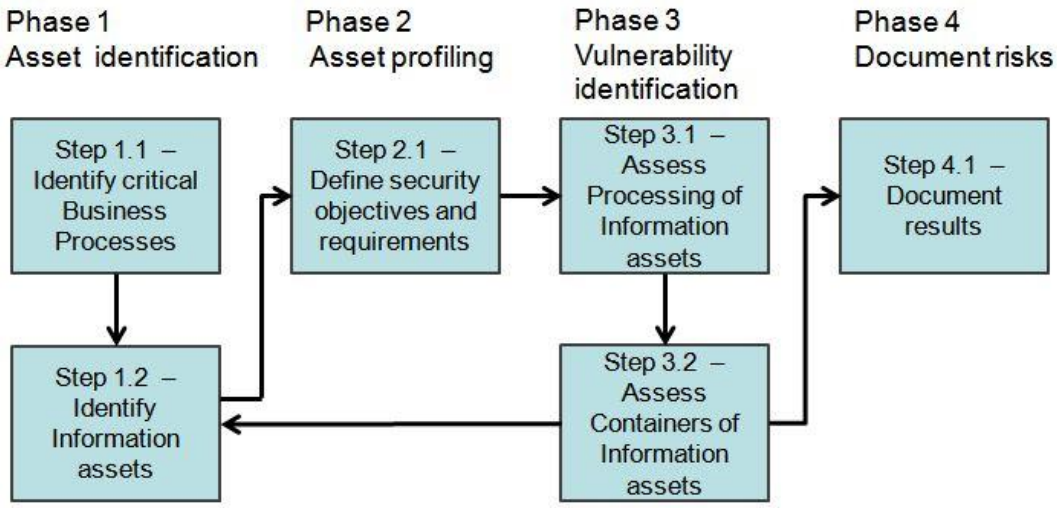

Figure 1. Security requirements risk assessment approach (SRA).

3.2. Running example

In the following, a real world example is used to demonstrate the applicability of approach in a practical and realistic environment. The example process (see Figure 2) is modelled in Business Process Modeling Notation (BPMN) (OMG, 2009). Due to page constraints not all intermediate results are presented.

Process model – online travel insurance quotation: A major part of the turnover of an insurance company is created via an online system offering travel insurance. The travel insurance for vacation, business trip and time abroad, is concluded when the customer has provided all data (name, address, e-mail, phone number, date of birth, travel details) and agreed to the terms and conditions of the company. Payments can be made via credit card or debit payment and afterwards the insurance contract is sent per email and post. The online system is a web application with a connected database storing all data about the contract, which has an interface to a third-party service to verify credit card and bank account data as well as to the accounting system for payment processing. As this is an example for illustration purposes, it is already known (before applying the approach) that the online system has a code injection problem when personal data is entered (at process activity 3 '- Display product details ...'), and an encryption problem at the interface with the third-party service (at process activity 4 'Verify personal and payment data'). In addition, the information technology (IT) continuity management process is not documented and tested.

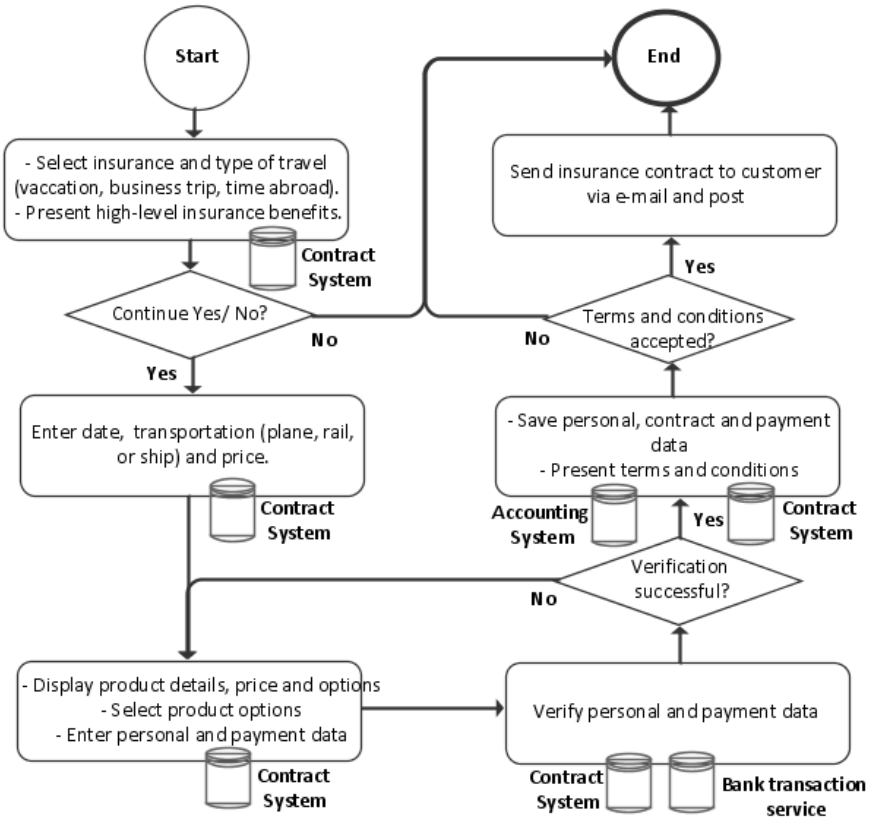

Figure 2. BPMN process model: Online travel insurance quotation

a. Asset identification phase

The objective of this phase is to identify the critical business processes (step 1.1) of an organisation and the information assets (step 1.2) of these processes. The criticality of the business process can be determined by the objective and output of a process and its value for the organization (e.g. a business impact analysis, where critical functions of a organization are identified whose disruption is regarded as unacceptable, can be used). Criteria and indicators for identifying information assets are the processes

decision points and process activity descriptions. The online travel insurance quotation process was identified as critical with customer and payment data as information assets.

b. Asset profiling phase

In the online travel insurance quotation process example, the following information assets were identified: customer and payment data. Amongst the information asset-related security requirements, it is distinguished between processing and the containers of information assets. For the processing of information, a security objective level is defined: low (L1), medium (L2), high (L3); for integrity (I), confidentiality (C) and availability (A), specifying the type of security needed (see Table I). For information asset containers, one has to define security requirements for the systems, organization and physical surroundings, considering the security objective level, as well as the essential IT security processes designated guaranteeing the protection of the asset (see Table I, second row from the top). The container security requirements refine the processing security objectives and describe what should be protected, as well as the concrete implementation. The artifacts used include the companies' security policy, organizational procedures, as well as security best practices for the definition of the requirements and IT security processes.

Information asset: Customer data		**Integrity**	**Confidentiality**	**Availability**	**IT Processes**
Processing	Data	I-L2	C-L2	A-L3	n/a
Containers	Primary Systems (PiSys)	Address data has to be verified in the system. Data in the system should be protected against unauthorized access and modification. 192-bit AES encryption if data is transfered	Access should be given only to company people. Changes have to be logged.	Within one business day	Access management (authorizations) IT security management (Seccurity of systems) Continuity management and disaster recovery Change management
	Organisation People Process	Personnel entering data should verify their entries as well as the data received.	People of the departments should be aware of confidentiality.	Core people within one business day.	Access management IT security training IT security policy
	Physical	none	Documents should be locked away and disposed of securely.	Within one business day.	IT security training Facility management Business continuity management

TABLE I. INFORMATION ASSET SECURITY REQUIREMENTS

c. Vulnerability identification phase

First, the degree of each implemented security functions of the process are evaluated and compared with the information assets' processing level requirements (1). Secondly, the information assets' containers (2) (systems, actors and environment) are evaluated with regard to the information assets' security requirements.

Evaluation of processing of information assets

One starts to determine where the information assets in the process are created, processed or transmitted. These locations are defined as entry (EP), process (PP) and communication (CC) points (see Figure 3). Entry points (EP) describe activities where information available is made processable by its entry into a system. Process points (PP) describe activities where data are permanently saved electronically, or modified (processed). Communication channels (CC) describe activities where data between process activities are transmitted. The EP, PP and CC of information assets were identified by keywords (e.g., enter, save, send) of process activity descriptions. Secondly, for each EP, PP and CC the degree of security function implementation – such as access control (AC), authorization (A), data input validation (D), communication (C) and encryption (E) - is determined, according the levels in Table II. Then, the security function implementation rating is compared against the processing requirement of the information assets at each EP, PP and CC, using a rule set representing a knowledge base. For example, the rating of access control at EP1 (Entry Point 1, rated as AC0 (Access Control level 0)) related to customer data is evaluated against the information assets security objective rating integrity level 2 using the rule set. The rule set represents security expert knowledge, considering both the security function and any objective level dependencies, and is implemented as PROLOG - a logic programming language - facts and rules. Due to space limitations any rule set used, or the interim results of the ratings are not included. The rating for an EP/PP and CC can be sufficient (ok), insufficient (nok), not/applicable (n/a) or unknown (u). Only for the security objective availability, different evaluation criteria were used - such as "level" and "measure". With "level", it is evaluated how often availability requirements were met in the past, and "measure" represents the implemented continuity measures. In the example in this paper (see Figure 4) only CC3 was rated as nok because of the missing data encryption.

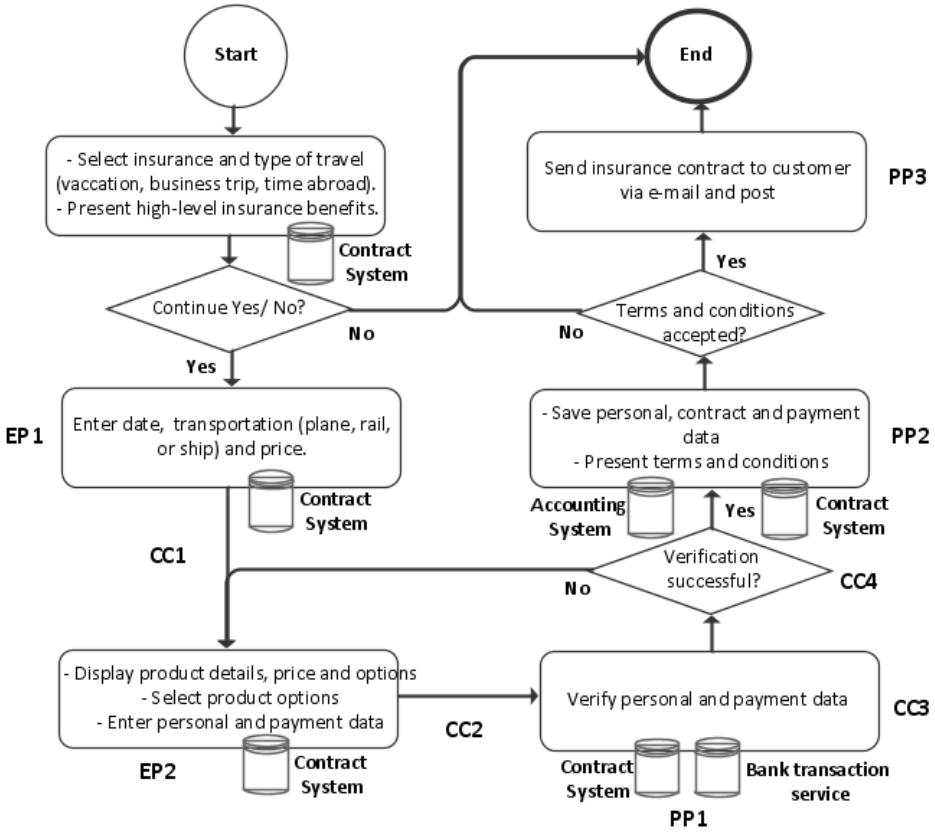

Figure 3. BPMN process model: Online travel insurance quotation with identified data process points

EP/PP/CC security implementation						
Access control	Authorization	Data input validation	Communication	Encryption	Level	Measure
AC0: Unauthent. user	A0: None	D0: None	C0: External unauthenticated partner	E0: None	L0: Never met	M0: none
AC1: Internal user	A1: Read	D1: Manual	C1: External authenticated partner	E1: Weak encryption	L1: Partially met	M1: Cold standby
AC2: Authent. user	A2: Execute/ process	D2: Downstream validation	C2: Internal network partner	E2: Standard encryption	L2: Partially not met	M2: Hot standby
AC3: System user	A3: Write/ update	D3: Value verification	C3: Internal authenticated partner	E3: Strong encryption	L3: Always met	M3: Redundancy
	A4: Full control	D4: Value verification and completeness				M4: Cluster
EP/PP/CC rating						
Not applicable (n/a), Unknown (u), insufficient (nok), sufficient (ok)						

TABLE II. EP, PP, CC RATING CRITERIA

Evaluation of containers of information assets

The containers' security requirements are evaluated by the security expert at each process activity where data processing (at EPs and PPs) takes place. CCs are evaluated between activities and evidence for security requirement adherence can be gathered from the system configuration/specification, the

company's security policy, process documentation or examples of implementation. IT processes are evaluated by system testing and process performance documentation reviews. In the example in this paper, the PiSys at EP2, PP1 and CC3 were evaluated as 'nok' because of the incorrect system implementation - the data modification via code injection and the missing data encryption. Furthermore, at CC3, payment data processing was affected by the encryption issue and therefore rated as 'nok'. The IT process review for customer data at the contract system resulted in the IT continuity process as a whole being rated as 'nok', because documentation and testing of the continuity process was missing.

Figure 4 illustrates the BPMN order process' evaluation results, for processing as well as for container security requirements. A BPMN textual annotation is used to document the evaluation results at every process activity, and a BPMN data object for information assets to show consolidated results.

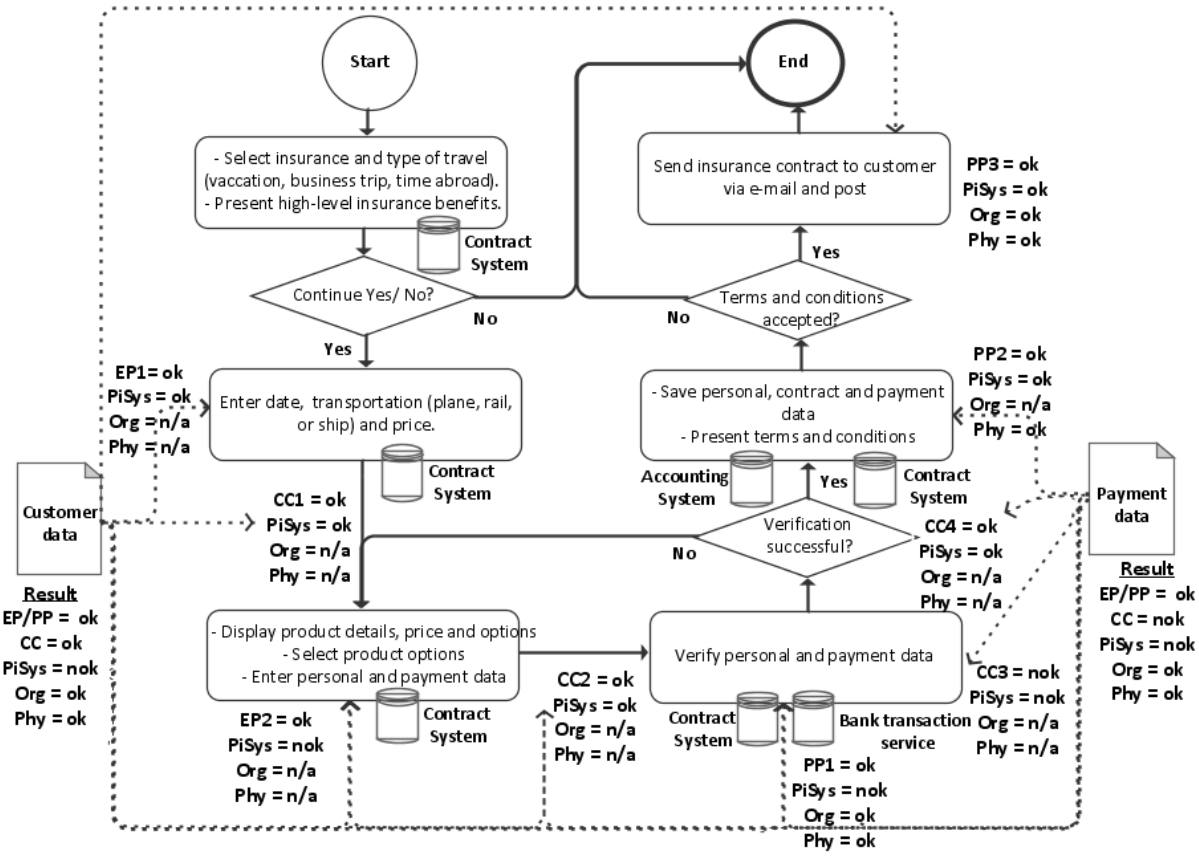

Figure 4. BPMN process model: Online travel insurance quotation process with evaluation information

d. Risk result documentation phase

At the end of the assessment, the risk results of the assessed information assets at the business processes are consolidated and presented as a matrix with the information asset at risk as the x-axis and the business/security process and issue identified as the y-axis. By this presentation, an overview of the information asset at risk at the different business/security processes can be indicated. At the online travel insurance quotation process, customer and payment data are vulnerable to code injections and encryption

is missing. Additionally, the security process performance of the IT continuity management process was evaluated as insufficient, affecting both information assets.

4. VALIDATION AND DISCUSSION

This chapter presents the validation of the approach by testing and a controlled experiment.

4.1. Vulnerability identification accuracy

With testing on real world examples, it has been verified that the approach is reliable (to produce the same results) and accurate (conformity to the results), determining vulnerabilities.

Context: IT security risk assessments are performed by two security experts at subsidiaries of a global insurance company, lasting one week at a maximum. The approach used is based on NIST SP 800-30 (Stoneburner et al., 2002) using COBIT (ITGI, 2007) control objectives and ISO/IEC 27001 (ISO, 2005a). IT staff are interviewed about security, and security scanning is conducted on systems. Security subject areas are selected based on importance, compliance requirements and common vulnerabilities. Systems used, underlying infrastructure, and the systems management are all examined; risks are determined and qualified by their significance (low, medium or high). The approach is performed along the NIST SP 800-30 risk assessment process. Threat- /Vulnerability identification and control analysis are performed by using vulnerability scanning tools, vulnerability lists and selected COBIT (ITGI, 2007) and ISO/IEC 27001 (ISO, 2005a) control objectives, evaluating implementation of controls. This approach is called the audit/risk assessment approach (ARA).

Proceeding: Both the ARA and the security requirements approach (SRA) proposed in this paper were applied, see section 3 for details, to a set of business processes (claims, accounting and underwriting) and systems of three distinct insurance entities. Each of the entities' IT departments operates directory, file, e-mail and application servers, as well as their internet access, and is connected to the corporate network; headquarters provide guidelines for IT security and system standardization. Each local IT department consists of about 20 to 30 people responsible for service desk, desktops and server operations. Application development does not take place. Business processes were available for the evaluated processes and process activities were similar because of the business model, but the level of detail and modelling of the processes differed between entities. At the first entity, the ARA and SRA were applied successively, twice, by one assessor. The ARA was applied successively by two experienced assessors, and the SRA by an experienced one and a naïve one. At the second and third entities, the ARA and SRA were performed by the same people - now acting as team. The teams did not change and they conducted the assessments subsequently at the three entities. The ARA and SRA teams had to specify the significance for the issues identified. There was no interaction between the teams after each assessment.

Results: At the end of each assessment, all results of the ARA and SRA were collected and common risk identifiers created to be able to compare results and facilitate easier result presentation. These common

risk identifiers were created by the area and issue identified in the ARA. Tables III, IV and V represent the assessment results of the ARA and SRA at the three entities by these common risk identifiers. Each table presents the issues identified at the entities by business areas, whether the issues was identified at the ARA or SRA by a 'Yes' or 'No', and the significance of the issue by a low, medium or high rating of the assessor(s). Any differences in the significance rating of the assessors were resolved by taking the highest rating. Table III contains the ARA and SRA assessments results of four assessors while tables IV and V contain the ARA and SRA assessment results of the two different assessment teams. Furthermore, for comparison reasons, the percentages and number of identified and unidentified vulnerabilities (with the rating of the ARA/SRA) were determined as well as the relative accuracy of the approaches at the three entities (see Table VI and discussion section).

Company 1 Results	**ARA**	**ARA**	**Significance**	**SRA**	**SRA**	**Significance**
1. Claims area						
1.1 The claims specialist has unrestricted access in the claims system.	Yes	Yes	Medium	Yes	Yes	High
1.2 There are no claims limits set up in the system.	No	No	-	Yes	Yes	High
1.3 There is no authorization activity in the process.	No	No	-	Yes	No	High
2. Accounting area						
2.1 Accountants can authorize bookings in the system but should not be possible.	No	No	-	Yes	No	High
2.2 Data transfer between the bank and the company is insecure as only a weak encryption is used.	Yes	Yes	Medium	Yes	Yes	Medium
3. Underwriting area						
3.1 There is no treaty data verification in the treaty system.	No	No	-	Yes	Yes	Low
4. General issues						
4.1 The operating system of the accounting system misses several patches.	Yes	Yes	High	Yes	Yes	Medium
4.2 The firewall is not properly configured; websites are not blocked.	Yes	Yes	Medium	No	No	-
4.3 Unused and active administrative accounts in MS Active Directory.	Yes	No	Low	No	No	-
4.4. Staff are not aware about IS threats.	Yes	Yes	Low	Yes	Yes	Low
4.5 There is no appropriate disaster recovery and business continuity documentation.	Yes	Yes	Medium	Yes	Yes	Medium
4.6 Paper documents were not securely stored in the Claims Department.	Yes	Yes	Low	Yes	Yes	Medium
4.7 Internal oral communication in the claims process was identified as not secure but assessed as uncritical.	No	No	-	Yes	No	Low

TABLE III. COMPANY 1 RESULTS

Company 2 Results	ARA	Significance	SRA	Significance
1. Claims area				
1.1 The claims specialist is able to release claims without authorizations in the system.	No	-	Yes	High
1.2 Process of claims data entry is inappropriate due to missing claims information.	No	-	Yes	High
1.3 Used spreadsheets for claims calculation - no access and change controls.	No	-	Yes	Medium
1.4 Claims data received were not properly checked.	No	-	Yes	Medium
2. Underwriting area				
2.1 Missing alignment between Underwriter and Actuarial services for contract pricing.	No	-	Yes	Medium
2.2 Broker approval process was to work as designed.	No	-	Yes	Medium
2.3 Missing authorization for underwriting policy deviations	No	-	Yes	High
3. General issues				
3.1 Weak VPN connection used by IT staff.	Yes	Medium	No	-
3.2 No updated disaster recovery plan.	Yes	Medium	Yes	Low
3.3 No testing of the BCM/DR activities.	Yes	Medium	Yes	Medium
3.4 System access approval process not adequate.	Yes	Medium	Yes	Medium
3.5 Daily data centre operations procedure not adhered to.	Yes	Medium	Yes	Medium
3.6 Unused and active administrative accounts in MS Active Directory.	Yes	Low	No	-
3.7 Data owner not aware of responsibilities.	Yes	Low	Yes	Low
3.8 Unused and active accounts in the HR application.	Yes	Medium	No	-
3.9 Paper documents were not securely stored.	Yes	Low	Yes	Low
3.10 No audit trail logging activated on database level.	Yes	High	No	-

TABLE IV. COMPANY 2 RESULTS

Company 3 Results	ARA	Significance	SRA	Significance
1. Claims area				
1.1 There is no authorization activity in the claims process.	No	-	Yes	Medium
2. Underwriting area				
2.1 Review and release of quotations in the system were not in line. No system-supported authorization process.	No	-	Yes	High
2.2 Inaccurate data from systems are used in the expected loss ratio studies.	No	-	Yes	High
2.3 Inappropriate use of spreadsheets for the calculation of premiums.	No	-	Yes	High
2.4 Local actuary model not aligned with central model.	No	-	Yes	Medium
3. General issues				
3.1 Shared account used for the online banking system	Yes	High	Yes	Medium
3.2 The operating systems for various servers are missing several	Yes	High	Yes	Medium

patches.				
3.3 No business continuity and disaster recovery plan in place	Yes	Medium	Yes	Medium
3.4 Unused and active administrative accounts in MS Active Directory.	Yes	Medium	No	-
3.5 No user access lists for local applications.	Yes	Low	Yes	Low
3.6 Unused and active accounts in the HR application	Yes	Medium	No	-
3.7 Paper documents were not securely stored.	Yes	Low	Yes	Low
3.8 No configuration management existent	Yes	Medium	Yes	Medium
3.9 Weak passwords for the backup recovery tool	Yes	Medium	No	-
3.10 The security incident process was not adhered to	Yes	Medium	Yes	Medium
3.11 Confidential information exchanged via internet	No	-	Yes	Medium

TABLE V. COMPANY 3 RESULTS

	Company 1		**Company 2**		**Company 3**	
No. total identified vulnerabilities	13		17		16	
	ARA	**SRA**	**ARA**	**SRA**	**ARA**	**SRA**
No. identified vulnerabilities	8	11	10	13	10	13
Relative accuracy on total identified vulnerabilities in %	62%	85%	59%	76%	63%	81%
Overlap between ARA and SRA – no. / in %	6 / 46%		6 / 35%		7 / 44%	
No. identified high vulnerabilities (in %)	1 (12%)	4 (36%)	1 (10%)	3 (23%)	2 (20%)	3 (23%)
No. identified medium vulnerabilities (in %)	4 (50%)	4 (36%)	6 (60%)	7 (54%)	6 (60%)	8 (62%)
No. identified low vulnerabilities (in %)	3 (38%)	3 (28%)	3 (30%)	3 (23%)	2 (20%)	2 (15%)
No. unidentified high vulnerabilities	3	0	3	1	3	0
No. unidentified medium vulnerabilities	0	1	4	2	3	3
No. unidentified low vulnerabilities	2	1	0	1	0	0

TABLE VI. OVERVIEW OF RESULTS

4.2. Vulnerability identification errors

To demonstrate that vulnerability identification errors occur and can be resolved by using security requirements, a controlled experiment was conducted included in a survey about security risk assessment procedures at an information security conference of professionals in the 'D-A-CH' region (Germany, Austria, Switzerland). The conference was about information security trends, threats and assessments. In the controlled experiment, participants had to assess the risks of a constructed example. Both the survey and controlled experiment were administrated by the present researchers. Because of space restrictions, the detailed controlled experiment description provided to the participants is not included in the paper.

Design: In the controlled experiment, each third of the conference participants (in total 55 security professionals) had to identify risks in a constructed example based on threats; based on threats and a business process model; and based on threats, security requirements and a business process model

respectively. Each third of the participants were provided randomly with one of three alternative sets of information representing the variables of the experiment. In case A (12 of 20 distributed forms were evaluable) a risk/threat description was provided, in case B (13 of 15 distributed forms were evaluable) the risk/threat description with a business process model was provided and in case C (11 of 20 distributed forms were evaluable) the risk/threat description with security requirements and a business process model were provided. The participants had to determine risks based on the information available. In cases A and B there were two predefined risks and in case C there were three additional predefined risks (see Table VII, risks 1 to 5) which was described in the threat (risks 1 and 2) and security requirement (risks 3,4 and 5) description.

Procedure: The controlled experiment was conducted with all 55 security professionals of the conference in a closed room and for the completion of the risk assessment, 30 minutes were available. A closed room was used so as not to disturb participants by any other people, or those leaving the experiment early. Interaction with other participants was not allowed and the survey instructor's involvement was limited to questions on how to fill out the template. All participants were security professionals responsible for information security in their companies, or security consultants and therefore knowledgable about security risks.

Results:

	Identified Risks in percentages		
	Case A	**Case B**	**Case C**
Analysed responses	**12**	**13**	**11**
Predefined Risks identified			
1.Data integrity (in example A, B and C)	100%	100%	73%
2. Data confidentiality (in example A, B and C)	67%	85%	91%
3. Process design data confidentiality access control (only example C)	8%	0%	45%
4. System availability (only example C)	100%	85%	100%
5. Process design authorization (only example C)	0%	0%	20%
6. Other identified risks (in example A, B und C)	75%	77%	55%

TABLE VII. EXPERIMENT RISK ASSESSMENT RESULTS

In case A the participants identified the predefined risks one and two by 100% and 67% (see table VII). All participants (100%) identified an availability risk that was not present; three out of four participants identified multiple other risks that were not present. In case B, predefined risks one and two were identified by 100% and 85% of participants, respectively. The non-existent availability risk was now only identified by 85%, but three out of four participants also identified multiple other risks that were not present. In case C 75% and 91% of participants identified the predefined risks one and two respectively, and 45%, 100% and 20% recognised risks three to five. Other risks were identified by 55%.

4.3. *Discussion of the results*

Vulnerability result accuracy at the ARA and SRA

To compare accuracy, one must know the true value. But as one does not know all existing vulnerabilities in these real world examples, it is hypothesised that all identified vulnerabilities in both approaches represent the relative accurate value. Whether all existing vulnerabilities are resolved cannot be verified, as a natural language for security requirements is used and the assessment is a manual process which is error-prone.

The *relative accuracy and significance of vulnerabilities* is used to determine accuracy. The *relative accuracy* varies between 18% and 23% higher accuracy for the SRA in all 3 cases, and is always constant above 76%. The SRA reliably identifies more vulnerabilities than the ARA. The overlap of 35-46% of the same identified vulnerabilities at the ARA and SRA with regard to the total number of vulnerabilities is attributed to the fact that the SRA identifies more process security issues whereas the ARA is more technically-focused. Using system scanning tools would improve identifying technical issues in the SRA, but tool-based vulnerability identification is time-consuming and momentum is lost (Caralli et al., 2007).

Further on, the *vulnerabilities' significance* using a distribution analysis was analysed. On average, 78% and 71% of all identified vulnerabilities are rated high or medium by SRA and ARA respectively. The risk significance distribution lies within the expected range of other approaches (Buyens et al., 2007) as well as the ARA result distribution within the 5-year historic data of 24 assessments with a higher tendency for low ratings as reported by others (Buyens et al., 2007). This study on the distribution of risk results indicates that assessment methods behave differently in the classification of threats. However, the study examined not whether one of the approaches has identified significantly more threats as another approach. The total number of unidentified vulnerabilities shows that the ARA missed 9 (20%) and the SRA one (2%) high-rated vulnerabilities, out of a total of 46. With the SRA approach a high accuracy on business process-related issues, as well as high-rated vulnerabilities can be achieved. Any other developed approaches would not perform better, as they are based on assessments standards of section 2 using security best practices and vulnerability lists for vulnerability identification, like in the ARA approach. Asset-specific security requirements are not evaluated to determine accuracy by these approaches. With the SRA, there are 15-28% low-rated vulnerabilities which one would not have expected because of the security requirements definition only identifying significant ones.

An *inter-rater reliability analysis* using Cohen's Kappa (Cohen, 1960) was performed for the ARA and SRA results at company one, determining consistency between raters, and was found to be 0.45 for the SRA and 0.51 for the ARA. This ratings represent a moderate agreement (Landis and Koch, March 1977) for both raters in both approaches, indicating the consensus was more than due to chance. In general, it is difficult to attain an almost perfect agreement between raters for risk assessments as the risk assessment

procedure to be followed is an informal one, relying on the assessors' experience and natural language descriptions of vulnerabilities and security requirements.

For the comparative analysis between the ARA and SRA results, one risk identifier had to be created and assigned which could have influenced the results of both approaches. This affects both approaches, assuming that it holds no advantage for either one of the approaches. One has to be aware that the SRA in this paper was tested only in one business sector at three companies. This may prevent generalizations, to some degree, for other business sectors. But the sample size is not unusual for this type of research, as often only one real world example is used by other researchers.

Vulnerability identification errors in the controlled experiment

The *experiment risk results* show that in all three cases - A, B and C - other risks were identified by between 55% and 77% of the participants (see table VII). In case B, the process model information supported study participants by identifying vulnerabilities more precisely; e.g., the increase of 18% in risk 2 and a decrease of 15% in risk 4. In case C, where security requirements were provided additionally, the identification of non-existent risks decreased (from 75% to 55%), but complexity negatively influenced the risk identification rate. Risk 5 was identified by 20% of participants and in risk 1, the rate decreased to 27% due to having to identify multiple risks. But in all cases, more vulnerabilities were identified as existent because assessors used tacit information and knowledge about security requirements as well as vulnerabilities.

The *response rate* was 60% in cases A and C but 87% in case B. Some of the forms were not filled or completed in a way so that results were not usable. The process model supported the participants to be able to evaluate risks, represented by a higher return rate. Case A was unusual as the risk description was represented clearly and easy to understand. The low response rate in case C can be attributed to the complexity of the risk assessment example as the variable of the controlled experiment had to be changed. In case C, the variable of the controlled experiment, the predefined risks, caused complexity. Additional risks in case C had to be created in comparison to A and B, to verify whether participants can identify vulnerabilities by the security requirement definition and not only by the risk description. This caused the accuracy of risks 1 and 2 to decrease slightly, as well as other risks being identified in case C.

The *error rate* - defined as non-existent risks identified per participant in the experiment - was: in case A=2.1; in B=1.6; and in case C=0.55. A participant in case A identified 1.5 times as many non-existent additional risks than one in case C. The business process model and security requirements provided helped the participants to identify risks more accurately - identifying the correct set of risks in the experiment.

The experiment participants had various *competence levels* in risk analysis and security assessments, which were determined by the survey beforehand, and therefore, participants were well aware of risk assessment concepts.

5. RELATED WORK

In early risk assessment approaches, the idea of using business processes was introduced to avoid focusing solely on technical security issues (CCTA, 1987, Halliday et al., 1996, Rainer et al., 1991). Later, annual loss expectancy (Suh and Han, 2003), loss of disruption (Neubauer et al., 2005) and business goals (Khanmohammadi and Houmb, 2010) began to be used to determine the criticality and importance of vulnerabilities in terms of losses or interruption. In these approaches the impact of a given vulnerability is determined but not the security required.

Approaches, like Méthode Harmonisée d'Analyse de Risques (MEHARI) - Harmonised Risk Analysis - (CLUSIF, 2010) or the Livermore Risk Analysis Methodology (Guarro, 1987), use risk scenarios to determine risks. A risk scenario comprises a threat, frequency and impact and is constructed by determining exactly what could befall a system. Mostly threat lists or security best practices are used for describing vulnerabilities in risk scenarios; these are then evaluated against the implementation of security controls. Several other approaches describe organisation-agnostic security solutions to be implemented and the security principles to be applied as well as common threats and vulnerabilities. For example, Control Objectives for Information and Related Technologies (COBIT) (ITGI, 2007), Standard of good practice for information security (ISF, 2005), Baseline Protection Manual (BSI, 2008), Generally Accepted Information Security Principles (GAISP) (ISSA, 2004) or ISO/IEC 27002 (ISO, 2005b). In CORAS (Stølen et al., 2002), a Platform for Risk Analysis of Security Critical Systems, threat and vulnerability modelling alongside with threat diagrams and structured brainstorming is used to identify risks. These approaches suggest applying common security principles or security best practices, or using modelling. They do not determine and evaluate specific security needs of assets to identify risks.

Over time security requirements were proposed (Gerber and von Solms, 2005, Gerber et al., 2001) for determing security controls with regard to the security needs. In the approaches of Innerhofer-Oberperfler and Breu (Innerhofer–Oberperfler and Breu, 2006), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) (Alberts et al., 2003), OCTAVE Allegro (Caralli et al., 2007), Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) - Expression of Needs and Identification of Security Objectives - (ANSSI, 2010) security requirements are used to determine the criticality and impact of vulnerabilities as well as for the selection of security solutions. In these approaches, "existing security checklists or standards like the Baseline Protection Manual [BSI03] or EBIOS [DCS05]" (Innerhofer–Oberperfler and Breu, 2006): 9) or "brainstorming about possible conditions or situations that can threaten an organization's information assets" (Caralli et al., 2007): 18) can be used for vulnerability identification. In NIST SP 800-30 (Stoneburner et al., 2002), vulnerability knowledge bases, system security testing and a security requirements' checklist are all used for vulnerability identification. The security checklist specifies only basic security standards (e.g., from government regulations or security directives). In EBIOS (ANSSI, 2010), threats are identified based on attack methods, and are then combined with security requirements to determine the impact. At Common Criteria for Information Technology Security Evaluation (CC, 2006), a product-oriented approach,

security requirements are used to evaluate a product or specification and to provide assurance that it meets the requirements. Although these approaches use security requirements, they determine only the impact of vulnerabilities by security requirements or only the requirements of a product; or using asset unspecific security standards.

In business process modelling approaches, security requirements are elicited and assigned to a business process, before the best security solution is identified by comparison with existing security catalogues or solutions (Herrmann and Herrmann, 2006, Roehrig and Knorr, 2004). These approaches focus on identifying and applying the best security solution for a business process, but not on evaluating the current security implementation.

On the other hand, in requirements engineering (RE) modelling languages are used to elicit, model and analyse security requirements based on security goals, threats or vulnerabilities identified beforehand. For example, catalogues of common weaknesses and attack patterns have been used to argue for security requirements (Franqueira et al., 2011) based on satisfaction arguments (Haley et al., 2008). Houmb et al, (2010) uses Common Criteria, Heuristics and UMLsec - an extension to the Unified Modelling Language (UML) - to elicit security requirements and map them to the design. However, RE approaches address security issues in the early phases of system development, their modelling languages unable to represent risk (Dubois et al., 2010) and are therefore not suitable for assessing a companies' risks.

6. CONCLUSION

Vulnerability identification errors occur as security experts have to rely on uncertain inputs as well as company-unspecific security practices. The controlled experiment results confirmed that up to 75% of the assessors identify one or multiple vulnerabilities that are not existent, as assessors make tacit assumptions about risks (Asnar and Zannone, 2008).

A key contribution of this work is that it was demonstrated that a security requirement and process model based approach can improve the accuracy of vulnerability identification. Security issues were identified 18% more accurately with a security requirements approach. Especially business-related security issues were identified more accurately, and these are more significant risks for the company (Khanmohammadi and Houmb, 2010). In a controlled experiment, vulnerability identification errors decreased by 20% using business process models and security requirements. The results show that the evaluation of security requirements in combination with process models helps to achieve a higher accuracy in analysing significant risks; such evaluations are hardly used for identifying vulnerabilities in current risk assessment approaches. But as the SRA was only tested in the insurance domain, results may not be applicable to other business sectors.

However, a security requirement-based approach has the advantage of making tacit domain security knowledge of the security expert and company-specific requirements explicit and being evaluated. This is usually not reflected in applying security best practices or vulnerability lists (Siponen and Willison, 2009).

More accurate vulnerability identification has the benefit of not applying any insufficient security measures and allows the creation of a statement about the security of a company - the presence and absence of vulnerabilities - which cannot be done by security testing (Wang, 2005). It is suggested to include the explicit evaluation of security requirements in risk assessment proceedings to achieve more accurate results. But vulnerability identification will still be an informal process relying on the security expert as well as on the interpretation of descriptions in natural language.

To our knowledge, no significant work has addressed vulnerability identification at business process activities explicitly evaluating security requirements of information assets.

7. REFERENCES

Alberts, C., Dorofee, A., Stevens, J. and Woody, C. (2003), 'Introduction to the OCTAVE approach', Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, USA.

ANSSI (2010), 'EBIOS 2010 - Expression of Needs and Identification of Security Objectives', ANSSI - Agence nationale de la sécurité des systèmes d'information. http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/

Asnar, Y. and Zannone, N. (2008), 'Perceived Risk Assessment', *in* '4th Workshop on Quality of Protection', ACM, pp. 59 – 63. http://qop-workshop.org/

ASNZ (1999), 'Australian/New Zealand Standard Risk Management ASNZ 4360:1999'.

ASNZ (2009), 'Australian/New Zealand Standard Risk Management AS/NZS ISO 31000:2009 - Risk Management – Principles and Guideline'.

BSI (2008), 'BSI-Standard 100-02: IT-Grundschutz Methodology', Federal Office of Information Security (BSI), https://www.bsi.bund.de/.

Buyens, K., De Win, B. and Joosen, W. (2007), 'Empirical and statistical analysis of risk analysis-driven techniques for threat management', *in* 'Proceedings of the Second International Conference on Availability, Reliability and Security', ARES '07, IEEE Computer Society, Washington, DC, USA, pp. 1034–1041. http://dx.doi.org/10.1109/ARES.2007.78

Caralli, R., Stevens, J., Young, L. and Wilson, W. (2007), 'Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process', Technical Report CMU/SEI-2007-TR-012; ESC-TR-2007-012, Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, USA.

CC (2006), 'Common Criteria for Information Technology Security Evaluation, September 2006 , Version 3.1', http://www.commoncriteriaportal.org/cc/.

CCTA (1987), 'CCTA Risk Analysis and Management Method', Central Computing and Telecommunications Agency (CCTA).

CLUSIF (2010), 'Mehari 2010 - Risk assessment and treatment Guide'. CLUSIF, Club de la Sécurité de l'Information Français. http://www.clusif.asso.fr/en/clusif/present/

Cohen, J. (1960), 'A coefficient of agreement for nominal scales', *Educational and Psychological Measurement* 20, pp. 37–46.

CSI (2009), '14th Annual CSI Computer Crime and Security Survey', Computer Security Institute (CSI), http://gocsi.com/.

Dubois, E., Heymans, P., Mayer, N. and Matulevius, R. (2010), 'A Systematic Approach to define the Domain of Information Security Risk Management', *in* 'International Perspectives on Information Systems Engineering', pp. 286–306.

Fenz, S. and Ekelhart, A. (2011), 'Verification, Validation, and Evaluation in Information Security Risk Management', *Security Privacy, IEEE* 9 (2), pp. 58 –65.

Franqueira, V. N. L., Tun, T. T., Yu, Y., Wieringa, R. and Nuseibeh, B. (2011), Risk and Argumentation: A Risk-based Argumentation Method for Practical Security, *in* '19th IEEE International Conference on Requirements Engineering', pp. 239-248. http://oro.open.ac.uk/28980/

Gerber, M. and von Solms, R. (2005), 'Management of Risk in the Information Age', *Computers & Security* 24, pp. 16–30.

Gerber, M., von Solms, R. and Overbeek, P. (2001), 'Formalizing Information Security Requirements', *Information Management & Computer Security* 9 (1), pp. 32 – 37.

Guarro, S. (1987), 'Principles and Procedures of the LRAM Approach to Information Systems Risk Analysis and Management', *Computers & Security* 6, pp. 493–504.

Haley, C. B., Laney, R. C. and Nuseibeh, B. (2004), 'Deriving Security Requirements from Crosscutting Threat Descriptions', *in* 'Proceedings of the 3rd international conference on Aspect-oriented software development', AOSD '04, ACM, New York, NY, USA, pp. 112–121. http://doi.acm.org/10.1145/976270.976285

Haley, C., Laney, R. and Moffett, J. (2008), 'Security Requirements Engineering: A Framework for Representation and Analysis', *IEEE Transactions on Software Engineering* 34(1), pp. 133–153.

Halliday, S., Badenhorst, K. and von Solms, R. (1996), 'A business approach to effective information technology risk analysis and management', *Information Management &Computer Security* 4 (1), pp. 19–31.

Herrmann, P. and Herrmann, G. (2006), 'Security requirement analysis of business processes', *Electron Commerce Research* 6, pp. 305– 335.

Houmb, S. H., Islam, S., Knauss, E., Jürjens, J. and Schneider, K. (2010), 'Eliciting Security Requirements and Tracing them to Design: an Integration of Common Criteria, Heuristics, and UMLsec', *Requir. Eng.* 15, pp. 63–93. http://dx.doi.org/10.1007/s00766-009-0093-9

Innerhofer–Oberperfler, F. and Breu, R. (2006), 'Using an Enterprise Architecture for IT Risk Management', *ISSA'06: Proc. Information Security South Africa Conference, South Africa, 2006.*

ISF (2005), 'The Standard of Good Practice for Information Security, V4.1', Information Security Forum (ISF), https://www.securityforum.org/.

ISO (2002), 'ISO Guide 73:2002 Risk Management', International Organization of Standardization (ISO).

ISO (2004), 'ISO/IEC 13335-1:2004 Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management', International Organization of Standardization (ISO).

ISO (2005*a*), 'ISO 27001:2005 Information technology - Security techniques - Information security management systems – Requirements', International Organization of Standardization (ISO).

ISO (2005*b*), 'ISO 27002 Information technology - Security techniques - Code of practice for information security management', International Organization of Standardization (ISO).

ISO (2009), 'ISO/IEC 31000:2009 Risk management — Principles and guidelines', International Organization of Standardization (ISO).

ISO (2011), 'ISO 27005:2011 Information technology - Security techniques - Information security risk management', International Organization of Standardization (ISO).

ISSA (2004), 'Generally Accepted Information Security Principles (GAISP)', Information Systems Security Association (ISSA), http://www.issa.org/.

ITGI (2007), 'Control Objectives for Information and related Technology (COBIT) Version 4.1', IT Governance Institute (ITGI), https://www.isaca.org/.

Khanmohammadi, K. and Houmb, S. H. (2010), 'Business Process-Based Information Security Risk Assessment', *Fourth International Conference on Network and System Security,* pp. 199–206.

Landis, J. R. and Koch, G. G. (March 1977), 'The measurement of observer agreement for categorical data', *Biometrics* 33 (1), pp. 159–174.

Mead, N., Hough, E. and Stehney, T. (2005), 'Security Quality Requirements Engineering (SQUARE) Methodology', Technical Report CMU/SEI-2005-TR-009, Software Engineering Institute (SEI), Carnegie Mellon University.

Neubauer, T., Klemen, M. and Biffl, S. (2005), 'Business Process-based valuation of IT-Security', *in* 'EDSER'05', ACM, St. Louis, Missouri, USA.

OMG (2009), 'Business Process Model and Notation (BPMN) FTF Beta 1 for Version 2.0', Object Management Group (OMG), August 2009, http://www.omg.org/.

Rainer, R.-K., Snyder, C. and Carr, H. (1991), 'Risk Analysis for Information Technology', *Journal of Management Information Systems* 8(1), pp. 129–147.

Roehrig, S. and Knorr, K. (2004), 'Security Analysis of Electronic Business Processes', *Electronic Commerce Research* 4, pp. 59–81.

Siponen, M. and Willison, R. (2009), 'Information security management standards: Problems and solutions', *Information & Management* 46, pp. 267–270.

Stevens, J. F. (2005), 'Information asset profiling', Technical Report CMU/SEI-2005-TN-021, Carnegie Mellon University.

Stølen, K., den Braber, F., Dimitrakos, T., Fredriksen, R., Gran, B. A., Houmb, S.-H., Lund, M. S., Stamatiou, Y. C. and Øyvind Aagedal, J. (2002), 'Model-based risk assessment – the CORAS approach', *in* 'NIK (2002) informatics conference, Kongsberg'.

Stoneburner, G., Goguen, A. and Feringa, A. (2002), 'NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems', National Institute of Standards and Technology (NIST), http://www.nist.gov.

Suh, B. and Han, I. (2003), 'The IS risk analysis based on a business model', *Information & Management* 41, pp. 149 – 158.

Verizon (2010), '2010 Data Breach Investigations Report', Verizon, http://www.verizonbusiness.com/.

Viera, A. J. and Garrett, J. M. (2005), 'Understanding Interobserver Agreement: The Kappa Statistic', *Family Medicine* 37 (5), pp. 360–363.

von Solms, R. and von Solms, B. (2005), 'From information security to ... business security?', *Computers & Security* (24), pp. 271–273.

Wang, A. J. A. (2005), Information Security Models and Metrics', *in* '43rd ACM Southeast Conference, March 18-20, 2005, Kennesaw, GA, USA.', Vol. 2 of *ACM-SE 43*, pp. 178–184.

zur Muehlen, M. (2005), 'Integrating Risks in Business Process Models', *in* '16th Australasian Conference on Information Systems, ACIS 2005 Proceedings, Paper 50, http://aisel.aisnet.org/acis2005/50', Sydney.